CP-10-01

Bob's sidekick (or how tripartite quantum correlations satisfy a type of rigidity and how this is useful for cryptography)

Anne Broadbent

University of Ottawa

Abstract

We present a variant of the two-prover interactive proof model, where the interaction pattern is limited to a 3-messages: setup-broadcast-response. By virtue of these limitations, classically, the model has the same power as the single-prover model where 3 messages are exchanged. In stark contrast, the quantum version of this model (which we call the 'Bob's sidekick' model) gives rise to monogamy-of-entanglement' (MoE) games, wherein the limitation on tri-partite entanglement hampers the provers, as compared to the single-prover case. We show how this limitation can be exploited for cryptographic purposes, for instance in "unclonable encryption" where the capacity of an adversary to copy a ciphertext is limited; this is achieved using an MoE game based on conjugate coding. What is more, we show the first rigidity theorem for this MoE game, which means that producing optimal winning statistics strongly constrains the quantum strategy of the provers. From this rigidity result, we derive a weak string erasure protocol, which implies bit commitment — in a model where classical bit commitment is impossible.

Based on joint work with Eric Culf (arXiv:2111.08081) and Sébastien Lord (arXiv:1903.00130).